

REMARKS/ARGUMENTS

1.) Claim Rejections – 35 U.S.C. §102(e)

The Examiner has maintained the rejection of claims 30-58 as being anticipated by Yamaguchi, *et al.* (U.S. Patent No. 5,604,807). The Applicant, again, traverses the rejections.

It must be remembered that anticipation requires that the disclosure of a single piece of prior art reveals every element, or limitation, of a claimed invention. Furthermore, the limitations that must be met by an anticipatory reference are those set forth in each statement of function in a claims limitation, and such a limitation cannot be met by an element in a reference that performs a different function, even though it may be part of a device embodying the same general overall concept. Whereas Yamaguchi fails to teach each and every limitation of claims 30-58, those claims are not anticipated thereby.

Claim 30 recites:

30. A method of establishing a session key shared between a first network element of a first network domain and a second network element of a second network domain, said first network domain comprising first cryptographic means and means for sharing a secret key with said second network domain comprising second cryptographic means, said method comprising the steps of:
 said first cryptographic means generating a freshness token;
 said first cryptographic means generating said session key based on said shared secret key and said generated freshness token;
 providing said session key (K) to said first network element;
 providing said freshness token to said second cryptographic means;
 said second cryptographic means generating a copy of said session key based on said shared secret key and said provided freshness token; and,
 providing said copy of said session key to said second network element. (emphasis added)

As presented in claim 30, the Applicant's invention is characterized by the use of a "freshness token" in methods, and systems, for providing secure communication between first and second network elements. A first cryptographic means associated

with a first network domain generates a freshness token, and then generates a session key **based on a shared secret key and the generated freshness token**. The session key (which is a function of the freshness token) is then provided to a first network element of the first network domain, and the freshness token is provided to a second cryptographic means associated with a second network domain. The second cryptographic means generates a copy of the session key based on the shared secret key **and** the received freshness token; the copy of the generated session key is then provided to a second network element. The first and second network elements can then communicate securely based on the use of the session key.

In rejecting claim 30 as being anticipated, the Examiner recites the elements thereof and asserts that they are all taught by Yamaguchi, referring to "Fig. 11-13, and col. 10 line 35 to col. 13 line 35." **The undersigned has reviewed the referenced portions of Yamaguchi, however, and can find no teaching of a "freshness token," much less any similar token used in the functions recited in claim 30.** Although Yamaguchi does describe use of a session key, it does not appear that it teaches a session key that is a function of a freshness token.

In responding to those prior arguments, the Examiner asserts that they are not persuasive for the following reasons:

Regarding Claims 1 applicants argued that the cited prior arts (CPA) [Yamaguchi et al. (D. S. Patent No.: 5,604,807)] *"Although Yamaguchi does describe use of a session key, it does not appear that it teaches a session key that is a function of a freshness token. And also does not have no teaching of a freshness token that comprises a random challenge".*

This is not found persuasive. The system of cited prior art teaches a system and method that has code gateway between server and network which receives **session key** from key delivery centre and shares it with client. The code communication system consists of multiple server and client connected to a delivery centre through a network. The key delivery centre generates a **session key**. The **session key** is used to establish a session to provide communication between the client and server. Before a session is established, the client outputs a code communication demand to a code gateway. The code gateway first receives the **session key** from the key delivery centre. A first gateway session key delivery section and a second gateway **session key** delivery section delivers this **session key** to the client. The **session key** is decoded in a second encipher-decoder in the code gateway. A **session key** acquisition section receives the **session key** from the code gateway. The received session key is stored in a **session key** holder. A synchronizing establishment unit establishes code synchronisation with the code gateway. A first session establishment section starts a first session with the server. Code synchronization with the

server is also performed during this session. A second session establishment unit establishes a second session and a code communication is performed.

As a result, the system of cited prior art does implement and teaches a system and method that relates to inter-network domain key management in communications systems, (Fig.11-13, and col.10 line 35 to col. 13 line 35).

Applicants clearly have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts.

Therefore, the examiner asserts that cited prior art does teach or suggest the subject matter broadly recited in independent Claims and in subsequent dependent Claims. Accordingly, rejections for claims 30-58 are respectfully maintained. (bold/italic emphasis added)

First, it is noted that the Applicant, in the previously-submitted arguments, identified several specific claim elements that are not explicitly, or implicitly, disclosed by Yamaguchi, and that the Examiner's response to those arguments again fails to identify those elements in Yamaguchi. For example, the Examiner's responsive argument repeatedly identifies Yamaguchi as teaching a "session key." In that regard, the Applicant agrees. Yamaguchi teaches a "shared session key." (Abstract: "the session key . . . [is] shared at the first and second terminals") Applicant's invention, however, is not characterized by a "shared session key," but a "shared secret key." Furthermore, according to Applicant's invention, a "session key" is generated by first cryptographic means **based on the shared secret key and a generated freshness token**. Therefore, not only is the "shared session key" disclosed by Yamaguchi not equivalent to the session key employed in Applicant's invention, it is also not analogous to the Applicant's "shared secret key." Moreover, the Examiner has still failed to identify any element in Yamaguchi that can be equated to the Applicant's "freshness token," much less the generation of that token by *first* cryptographic means, and the subsequent generation of the session key by *second* cryptographic means **based on the shared secret key and the freshness token**. Accordingly, the Examiner's response to Applicant's arguments again fails to point to specific teachings in Yamaguchi of each and every limitation of claim 30 and, therefore, that claim is not anticipated thereby.

The Applicant further notes that the Examiner's responsive arguments in the Final Office Action fail to address the additional arguments presented by Applicant with respect to claim 33. In the specific embodiment recited in claim 33, which is dependent

from claim 30, the freshness token comprises a random challenge, and the method of claim 30 further comprises the steps of:

said first cryptographic means generating an expected response based on said shared secret key and said random challenge;

providing said expected response to said first network element;

said second cryptographic means generating a response based on said shared secret key and said provided random challenge;

providing said response to said first network element; and,
said first network element authenticating said second network element based on a comparison between said expected response and said response. (emphasis added)

In rejecting claim 33, the Examiner recites the elements thereof and asserts that they are all taught by Yamaguchi, referring to "col. 10 line 35 to col. 11 line 50." The undersigned has reviewed the referenced portion of Yamaguchi, however, and can find no teaching of a freshness token that comprises a random challenge and which is employed in the functions recited in claim 33. Therefore, Yamaguchi also fails to anticipate claim 33.

Whereas independent claims 31, 42, 43, 51 and 55 include limitations analogous to those of independent claim 30 relating to a freshness token, those claims are also not anticipated by Yamaguchi. Similarly, whereas dependent claims 45, 53 and 57 limit the freshness token to a random challenge, further comprising limitations analogous to those of dependent claim 33, they are not anticipated by Yamaguchi. Finally, whereas claims 32 and 34-41 are dependent from claim 30; claims 44 and 46-50 are dependent from claim 42; claims 52 and 54 are dependent from claim 51; and claims 56 and 58 are dependent from claim 55, and include the limitations of there respective base claims, they are also not anticipated by Yamaguchi.

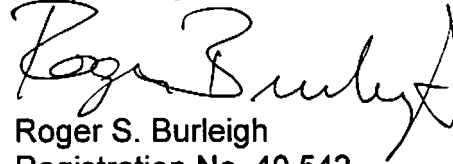
* * *

CONCLUSION

In view of the foregoing remarks, the Applicant believes all of the claims currently pending in the Application to be in a condition for allowance. The Applicant, therefore, respectfully requests that the Examiner withdraw all rejections and issue a Notice of Allowance for claims 30-58.

The Applicant requests a telephonic interview if the Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,



Roger S. Burleigh
Registration No. 40,542

Date: November 16, 2010

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024

(972) 583-5799
roger.burleigh@ericsson.com